AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Ryan P. Doyle, being first duly sworn, hereby depose and state as follows:

Introduction and Agent Background

1. I am a Detective Sergeant with the Newport Police Department ("NPD") and a Task Force Officer ("TFO") with the U.S. Drug Enforcement Administration ("DEA"). I have been a TFO since January 2021, and a Detective since 2014. Prior to becoming a Detective, I was a police officer with the Newport Police Department since 2007. As both a TFO and Detective, I have participated in investigations of narcotics trafficking and have conducted or participated in surveillances, the execution of search warrants, debriefings of informants and reviews of recorded conversations. Through my training, education, and experience, I have become familiar with the manner in which narcotics are packaged, distributed and transported. I am currently assigned to conduct investigations in the Providence District Office ("PDO") of the DEA. I have prepared numerous affidavits in support of applications for State and Federal search warrants. My duties include the enforcement of federal criminal laws, including controlled substance violations and money laundering, under Titles 18 and 21 of the United States Code.

2. As a TFO with the DEA, I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), in that I am empowered by law to conduct investigations and to make arrests for federal felony offenses. I am a participating member of the PDO which is comprised of

personnel from the DEA and DEA Task Force Officers (TFOs) from the Providence Police Department, Woonsocket Police Department, Cranston Police Department, NPD, Middletown Police Department, Warwick Police Department, Pawtucket Police Department, Rhode Island State Police, and the Amtrak Police Department. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

3. Drug trafficking is a business that involves numerous co-conspirators, from lower-level dealers to higher-level suppliers, as well as associates to process, package, and deliver the drugs and launder the drug proceeds. Drug traffickers often travel by car, bus, train, or airplane, both domestically and to foreign countries, in connection with their illegal activities in order to meet with co-conspirators, conduct drug transactions, and transport drugs or drug proceeds.

4. Based on my training and experience, I understand that illegal drug trafficking involves the local, interstate, and international movement of drugs to distributors and co-conspirators at multiple levels, and the movement of the proceeds of drug trafficking among multiple participants including suppliers, customers, distributors, and money launderers. Consequently, the location of drug traffickers and those working with them can be instrumental in identifying and intercepting shipments of illegal drugs and drug proceeds. Based on my training and experience, I know that illegal drugs and drug proceeds are often transported in motor vehicles and that drug

traffickers often coordinate drug trafficking activity through the use of cellular telephones. Drug traffickers often keep stashes of narcotics in their vehicles in the event of an unexpected opportunity to sell narcotics arises.

5. It is common for drug traffickers to own and/or use multiple phones of varying sophistication and cost to communicate with their various customers and suppliers. These phones range from sophisticated smart phones to cheap, simple, and often prepaid flip phones, known colloquially as "drop phones," for other text and voice communications. In addition to text and voice calls over cellular telephones, drug traffickers use digital communications applications such as text messaging platforms (including SMS and MMS), iMessage, WhatsApp, Telegram, Skype Messenger, Kik, Viber, Google Hangouts, social media applications, and other similar applications as well as via email.

6. I have become familiar with the ways drug traffickers communicate with each other and with their customers and suppliers; the coded language that is used by drug traffickers to disguise the criminal nature of their activities from law enforcement; retail and wholesale prices for varying quantities of narcotics; and methods of laundering drug trafficking proceeds. Additionally, based on my training and experience and my participation in other narcotics investigations, I have learned that it is common for drug dealers to "front," or provide on consignment, controlled substances to their customers. Drug traffickers will send photos or videos of or related to the drugs between the seller and the buyer, the negotiation of price, and discuss

whether or not participants will bring weapons to a deal. In addition, it is common for people engaged in drug trafficking to have photos and videos on their cell phones of drugs that they or others working with them possess, photographs of themselves with drugs and money and that they frequently send these photos to each other and others to boast about the drugs or facilitate drug sales.

7. I know that drug dealers will travel with their cellular telephones to places where they make drug deliveries to customers and to places where they store their drugs. I know that many wireless telephones store location information on phones and that services providers may be able to provide prospective phone location data for cellular telephones and other electronic devices. I also know that tracking the location of a drug dealer's cellular telephone can assist law enforcement officers with surveillance and lead to the location of drug suppliers and "stash houses."

8. In addition to keeping drugs in vehicles, I know that drug traffickers often maintain "stash houses" to store drugs, drug distribution centers, as well as proceeds. I know that drug traffickers also keep drugs and evidence of drug trafficking in their homes and businesses. I have participated in the execution of numerous search warrants at the residences of drug-traffickers. Based on my training and experience and familiarity with investigations into drug trafficking conducted by other law enforcement agents, I know the following and have found evidence of the following in the stash houses, homes and businesses of drug traffickers:

a. Drug traffickers often maintain a supply of drug and materials used to package drugs, such as packaging materials and scales. These items are often small enough to be easily hidden and thus may be kept at these locations, even if it is a business conducting other activity and even though the drug trafficker may live with others who may be unaware of his/her criminal activity.

b. Drug traffickers often keep proceeds of narcotics trafficking in safes and other places, as well as large amounts of United States currency, in order to maintain and finance their ongoing drug trafficking businesses, which operate on a cash basis.

c. Drug traffickers often maintain books, receipts, notes, ledgers, bank records, and other records relating to the manufacture, transportation, ordering, sale and distribution of illegal drugs. The aforementioned records are often maintained where drug traffickers have ready access to them, such as on their cell phones and other digital devices including tablets, personal and business computers.

d. Drug traffickers often keep the names, addresses, and telephone numbers of their drug trafficking associates on their digital devices, on their person, and in their residences and businesses. Drug traffickers often keep records of meetings with associates,

customers, and suppliers on their digital devices and in their residence and businesses, including in the form of calendar entries and location data.

e. It is common for drug traffickers to maintain personal property that tend to identify the person(s) in residence, occupancy, control, or ownership of the premises or vehicles. Such identification evidence is typical of the articles people commonly maintain at these locations, such as canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, utility and telephone bills, statements, identification documents, and keys.

Purpose

9. I submit this affidavit in support of an application for the issuance of search warrants authorizing the search of:

a. The residence located at 102 Sassafras Street apartment 1, Providence, RI ("TARGET PREMISE 1"), and 425 Public Street apartment 1, Providence, RI (TARGET PREMISE 2), (hereinafter referred to collectively as "TARGET PREMISES") as more particularly described in Attachment A-1 and A-2 for the items described in Attachment B-1 and B-2. I have viewed the TARGET PREMISES and am familiar with their appearance.

b. Rhode Island registration 1NG180 on a 2009 Toyota RAV 4 blue in color ("TARGET VEHICLE"), as more particularly described in Attachment A-3 for the items described in Attachment B-3. I have viewed the TARGET VEHICLE and am familiar with its appearance.

c. The person described as Marisol SANTIAGO (DOB [redacted]) (hereinafter referred to as "SANTIAGO" or "TARGET PERSON"), as more particularly described in Attachment A-4 for the items described in Attachment B-4, at whatever location she is found, regardless of SANTIAGO's location or proximity to the TARGET PREMISES, including any cellular telephones or digital storage devices she may have on her person.

10. For the reasons set forth below, I believe that SANTIAGO is a drug trafficker who is using the TARGET PREMISES and TARGET VEHICLE to store narcotics and/or narcotics proceeds, and further that SANTIAGO uses cellular telephones to carry out drug trafficking activities. I submit that there is probable cause to believe that the TARGET PREMISES and TARGET VEHICLE contain records and other evidence of the following offenses: conspiracy to distribute and possess with the intent to distribute fentanyl, in violation of 21 U.S.C. § 846, and possession with the intent to distribute fentanyl, in violation of 21 U.S.C. §§ 841 (a)(1) and (b)(1)(C) (collectively, the "TARGET OFFENSES"), and that the cellular telephones used by

SANTIAGO, the TARGET PERSON, contain evidence of the TARGET OFFENSES. More specifically, as will be discussed below, I submit that there is probable cause to believe that the TARGET PREMISES and TARGET VEHICLE will contain evidence of the commission of a criminal offense or evidence which is contraband, the fruits of crime, or things otherwise criminally possessed, or which is designed or intended for use or which is or has been used as the means of committing an offense in violation of the TARGET OFFENSES.

Probable Cause

11. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement agents. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter. I have also relied on information provided to the DEA by a Confidential Informant who I will only refer to as "CS." In order to protect CS's identity, I will refer to CS with a masculine pronoun regardless of CS's gender.

12. The CS has been providing information to the government since September 2024. The CS is currently cooperating to potentially receive a reduced or deferred sentence on a State narcotics charge. Information provided by the CS has been proven to be reliable, and the CS has not provided information that law enforcement later found to be untrue. The CS has criminal convictions that include robbery, heroin

possession, and possession of stolen property. This CS has been proven to be credible and has provided members of the DEA with information regarding several other narcotics traffickers, all of which has been proven to be true. The CS has not provided information to the DEA that has been false.

13. The DEA has been conducting an investigation into the fentanyl trafficking activities of an unidentified Hispanic male. This Hispanic male utilizes Marisol SANTIAGO to deliver and store the fentanyl. The DEA initially became aware of SANTIAGO's narcotics trafficking after the CS informed members of the DEA that he frequently purchases fentanyl from her. The CS explained that he contacts the Hispanic male and orders the fentanyl. The CS stated that the Hispanic male arranges the narcotics transaction and SANTIAGO arrives to deliver the fentanyl. The CS stated that the fentanyl is sold in blue wax bags which are bundled together in packs of 50 bags known as "bricks." A "brick" is 50 of the blue bags containing fentanyl bundled together. The CS stated that SANTIAGO operates a blue colored Toyota Rav4, RI registration 1NG180. This vehicle is registered to SANTIAGO at her residence, 102 Sassafras Street 1st floor (TARGET PREMISE 1).

14. Within the past few weeks members of the DEA have conducted surveillance of the TARGET PREMISE 1. During this surveillance members of DEA have observed SANTIAGO coming and going from the residence while operating the TARGET VEHICLE.

15. Over the past two weeks, DEA TFO Chad Souza and I met with the CS to prepare for a controlled purchase from SANTIAGO. Other members of the PDO set up surveillance of TARGET PREMISE 1 and noted that TARGET VEHICLE was parked in front. Members of the DEA maintained surveillance of the TARGET PREMISE 1 and TARGET VEHICLE. The CS called the Hispanic male who was utilizing Whatsapp number [redacted]. I overheard the phone conversation in which the CS ordered an amount of fentanyl bricks from the Hispanic male. The Hispanic male stated that SANTIAGO would meet the CS in a short time. Through a series of phone calls and Whatsapp messages between the CS and the Hispanic male, the CS eventually arranged to meet SANTIAGO in a prearranged location within the City of Providence.

16. The CS and his vehicle were searched prior to and after the controlled purchase. If the CS had any currency on him or within his vehicle, it would have been taken from him until after the purchase and then returned to him after the controlled purchase. The CS and his vehicle were searched to determine if he was already in possession of any narcotics, weapons and other contraband. The CS was not found to be in possession of narcotics, weapons, or other contraband during the search. The CS was provided with an amount of Official Advanced Funds ("OAF") to make the purchase.

17. Members of the DEA followed the CS to the prearranged location established for the deal and then remained under constant surveillance. Shortly before the scheduled meeting, members of the PDO observed SANTIAGO leave the TARGET PREMISE 1 in the TARGET VEHICLE. Members of the DEA followed SANTIAGO

directly to 425 Public Street in Providence RI, TARGET PREMISE 2. SANTIAGO was observed entering the front door and then a short time later observed exiting with a black bag in her hand. TARGET PREMISE 2 is known to members of the DEA as a money and narcotics "stash house" run by Cirila BEATO De GOMEZ. This information came from a large-scale drug trafficker who was arrested and debriefed several months ago.

18. SANTIAGO was then followed in the TARGET VEHICLE directly to the prearranged meet spot with the CS. After a quick meet, the CS and SANTIAGO drove away from the area. SANTIAGO was followed directly back to the TARGET PREMISE 1 and observed going inside.

19. The CS left the meeting location and members of the DEA followed him, under constant surveillance, directly back to a prearranged location. Once there, the CS turned over several "bricks" of fentanyl to me. The CS stated that he purchased the fentanyl from SANTIAGO utilizing the OAF. A search of his person and vehicle revealed that he was no longer in possession of the OAF or narcotics. I conducted a field test on a sample of the suspected fentanyl which was positive for the presumptive presence of fentanyl. The estimated gross weight of the fentanyl (including plastic packaging) was over 400 grams. The fentanyl was processed under DEA guidelines and later sent to the Northeast Regional Laboratory for confirmatory testing.

20. Over the past week members of the DEA have conducted surveillance of both TARGET PREMISES. During this surveillance members of the PDO observed

SANTIAGO coming and going from her residence, TARGET PREMISE 1, while operating the TARGET VEHICLE. Members of the DEA also observed at least one known narcotics trafficker come and go from 425 Public Street, TARGET PREMISE 2. This known trafficker was a close associate of the debriefed trafficker that provided credible information on this location.

21. DEA TFO Chad Souza and I met with the CS to prepare for another controlled purchase from SANTIAGO. Other members of the PDO set up surveillance of TARGET PREMISE 1 and noted that TARGET VEHICLE was parked in front. Members of the DEA maintained surveillance of the TARGET PREMISE 1 and TARGET VEHICLE. The CS called the Hispanic male on Whatsapp number [redacted]. The CS ordered an amount of fentanyl bricks from the Hispanic male. The Hispanic male stated that SANTIAGO would meet the CS in a short time at a prearranged location in the City of Providence.

22. The CS and his vehicle were searched with negative results for contraband. The CS was provided with an amount of OAF to make the purchase. The CS was then followed, under constant surveillance, to the prearranged meet location in the City of Providence.

23. A short time later TFO McGuire observed SANTIAGO leaving the TARGET PREMISE 1 and get into the TARGET VEHICLE. SANTIAGO was then followed directly to the prearranged meet location where she was observed meeting with the CS. After a quick exchange the CS and SANTIAGO were both observed

leaving the area. Members of the DEA followed SANTIAGO directly back to the TARGET PREMISE 1.

24. The CS was followed, under constant surveillance, back to a prearranged location. Once there, the CS turned over several "bricks" of fentanyl to me. The CS stated that he purchased the fentanyl from SANTIAGO using the provided OAF.

25. A search of his person and vehicle revealed that he was no longer in possession of the OAF or narcotics. I conducted a field test on a sample of the suspected fentanyl which positive for the presumptive presence of fentanyl. The estimated gross weight of the fentanyl (including plastic packaging) was over 400 grams. The fentanyl was processed under DEA guidelines and later sent to the Northeast Regional Laboratory for confirmatory testing.

26. Based on the above controlled purchases, I believe TARGET PREMISE and TARGET PREMISE 2 are locations where drugs are stored for distribution. I also believe that TARGET PREMISE 1 is a location where proceeds of drug trafficking can be located.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

27. As described above and in Attachments B-1 and B-2, this application seeks permission to search for records that might be found in the TARGET PREMISES, TARGET VEHICLE and on the TARGET PERSON, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard

drive or other storage media.[1] Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

28. Probable cause. I submit that if a computer or storage medium is found in the TARGET PREMISES, TARGET VEHICLE, and/or on the TARGET PERSON, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

[1] The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

29. Forensic evidence. As further described in Attachment B-1, this application seeks permission to locate not only computer files that might serve as direct

evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the TARGET PREMISES, TARGET VEHICLE, and/or TARGET PERSON because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating, or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user

accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g.,

internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is

necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

30. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be

necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

31. Because another person is believed to share the TARGET PREMISES as a residence, it is possible that the TARGET PREMISES will contain storage media that are

predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

32. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

33. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly

newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID."

During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law

enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time

the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises

and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

CONCLUSION

34. Based on the above, I submit that there is probable cause to believe that the TARGET PERSON, SANTIAGO, is committing the TARGET OFFENSES or possession with the intent to distribute controlled substances and conspiracy to possess with the intent to distribute controlled substances. I further submit that there is probable cause to search the TARGET PREMISES described in Attachment A-1 and A-2 for the evidence described in Attachment B-1 and B-2 the TARGET VEHICLE described in Attachment A-3 for the evidence described in Attachment B-3, and the TARGET PERSON described in Attachment A-4 for the evidence described in Attachment B-4.

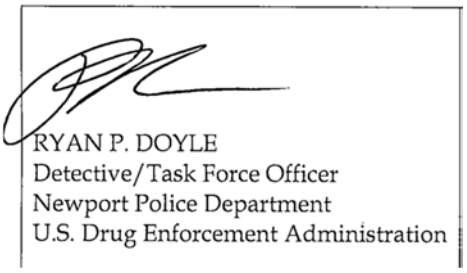
REQUEST FOR SEALING

35. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the affidavit, application, and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing

investigation into the criminal organization, as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

36. I, Ryan Doyle, having signed this Affidavit under oath as to all assertions and allegations contained herein, state that its contents are true and correct to the best of my knowledge, information, and belief.

Respectfully submitted,



RYAN P. DOYLE
Detective/Task Force Officer
Newport Police Department
U.S. Drug Enforcement Administration

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1. by: **Telephone** (specify reliable electronic means)

_____	_____
Date	Judge's Signature
_____	_____
City and State	Printed Name and Title

ATTACHMENT A-1

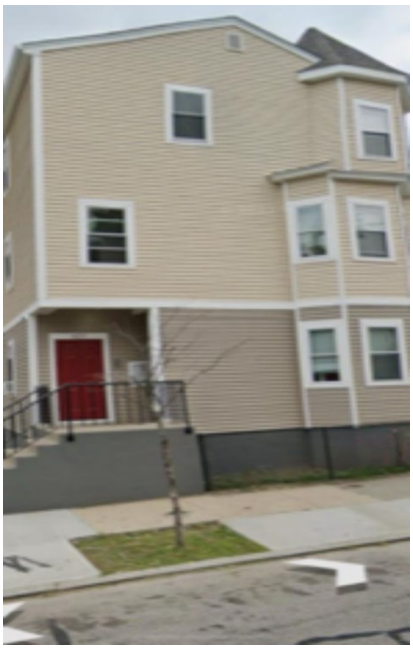
Premises to be Searched

The residence located at 102 Sassafras Street apartment 1 Providence, RI, TARGET PREMISE 1, (picture below), which is further described as a tan-colored multiple family residence with a black metal fence in front. The residence is a multiple family home and shares a structure with 104 Sassafras Street. The residence can be accessed through a front door facing Sassafras Street.

ATTACHMENT A-2

Premises to be Searched

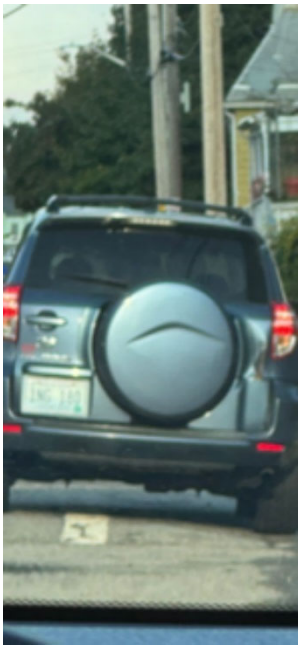
The residence located at 425 Public Street 1st, Providence, RI, TARGET PREMISE 2 (picture below), which is further described as a tan-colored multiple family residence with a maroon colored door. 425 Public Street has the number 425 affixed above the front door. The residence shares a structure with 427 Public Street. The residence can be accessed through a front door on Public Street Street.



ATTACHMENT A-3

Vehicle to be Searched

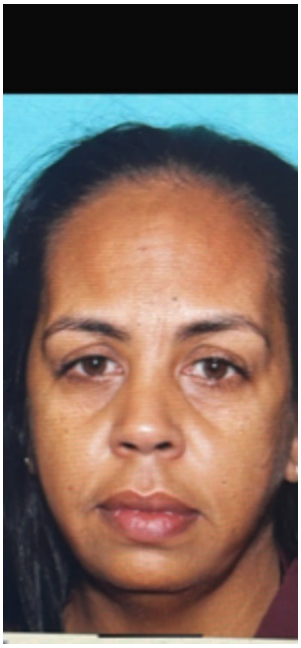
MARISOL SANTIAGO's blue 2009 Toyota Rav4 (TARGET VEHICLE), Rhode Island registration 1NG180, VIN # JTMZF33VX9D006957. This vehicle is registered to SANTIAGO at 102 Sassafras Street in Providence RI. (Picture below)



ATTACHMENT A-4

Person to be Searched

MARISOL SANTIAGO, is a Hispanic female, with black colored hair and brown eyes approximately 5' 6" in height and 160 lbs in weight. Her date of birth is [redacted] (Picture below).



ATTACHMENT B-1, B-2, and B-3

I. ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as a means of committing a criminal offense, namely violations of 21 U.S.C. § 841(a)(1); and conspiracy to possess with intent to distribute and/or distribute controlled substances, in violation of 21 U.S.C. § 846 ("TARGET OFFENSES").

1. Narcotics and narcotics paraphernalia.
2. Items and paraphernalia for the manufacturing, distributing, packaging, sale, or weighing of controlled substances, including scales and other weighing devices, plastic baggies, food saver sealing devices, heat sealing devices, balloons, packaging materials, containers, and money counters.
3. Items used in the packaging of currency for consolidation and transportation, such as money-counting machines, money wrappers, carbon paper, rubber bands, duct tape or wrapping tape, plastic wrap or shrink wrap, and plastic sealing machines.
4. Firearms.
5. Keys to 2009 Rav4.
6. Records and information[2] relating to the receipt, transport, storage, and/or sale of narcotics.
7. Records and information relating to banking and financial records of or relating to SANTIAGO any conspirators, and their nominees, assignees, or co-conspirators, including but not limited to bank statements, deposit tickets, deposit items, checks, money orders, cashier's checks, official checks, bank drafts, wire transfer instructions and receipts, checkbooks, check registers, passbooks, withdrawal slips, credit memos, debit memos, signature cards,

[2] As used in this Attachment, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks, backup drives, or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and digital and photographic form.

account applications, automatic teller machine receipts, safe deposit box applications, safe deposit box keys, pre-paid debit and credit cards, debit and credit card statements, charge slips, receipts, financial statements, balance sheets, income statements, cash flow statements, ledgers, journals, accounts receivable, accounts payable, leases, brokerage statements, and any other items evidencing the obtaining, disposition, secreting, transfer, or concealment of assets.

8. Records and information relating to the access and use of money service businesses, such as Western Union and/or Moneygram; online bank transfer services, such as Zelle, Venmo, or Paypal; and cryptocurrency accounts and cryptocurrency exchanges, such as BitCoin.
9. United States currency, money orders, or cashier's checks.
10. Records and information relating to any communications by, between and among, and/or relating to SANTIAGO and any conspirators, relating to the TARGET OFFENSES, including opening and access of bank accounts.
11. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show access, accounts with, and/or use of instant and social media messages (including Facebook, Facebook Messenger, Instagram, Pinterest, Snapchat, FaceTime, Skype, and WhatsApp), SMS and MMS text messages, iMessage, iCloud, and email accounts by SANTIAGO, and any conspirators. Records and information showing communications by, between and among, and/or relating to SANTIAGO, and any conspirators, that relate to the TARGET OFFENSES via any such accounts and communications platforms.
12. Records and information relating to Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations, including travel to banking locations.
13. Any records which document an association between and among SANTIAGO, and any conspirators, including social media accounts, photographs, and video and audio recordings.
14. Records and information records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with any co-conspirators involved in the TARGET OFFENSES, including calendars, address books, telephone or other contact lists,

correspondence, receipts, and wire transfer or fund disposition records, and communications relating to the same.

15. All records or documents evidencing or relating to foreign or domestic travel of SANTIAGO, or co-conspirators, including but not limited to airline tickets, tickets for other means of transport, credit card receipts, travel vouchers, hotel receipts, restaurant receipts, gas receipts, notes, schedules, other receipts evidencing travel, boarding passes, itineraries, luggage tags and receipts, frequent flyer statements and awards, car rental receipts and statements, photographs of travel locations, maps, written directions to a location, visas, passports, United States and foreign customs declaration receipts and forms.
16. Records and documents reflecting the purchase or lease of real estate and vehicles, precious metals, jewelry, or other items obtained with drug trafficking proceeds.
17. Identification cards, driver's license cards, passports, visas, and travel documents.
18. Records relating to the use, ownership, possession, and control of computers, tablets, cellular telephones, and/or other cellular and digital devices seized from SANTIAGO, internet service, or IP addresses associated with SANTIAGO;
19. For any computer, cellular or digital device, cellular telephone, and/or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information whose seizure is authorized by this warrant, including any cell phones (hereinafter, "DIGITAL DEVICE")[3]:
    a. evidence of who used, owned, or controlled the DIGITAL DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email

[3] The term "DIGITAL DEVICE" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile/cellular phones, tablets, server computers, and network hardware. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, external drives, RAM, flash memory, CD-ROMS, memory sticks, USB drives, and other magnetic or optical media.

contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the DIGITAL DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
c. evidence of the lack of such malicious software;
d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crimes under investigation and to the computer user;
e. evidence indicating the computer user's knowledge and/or intent as it relates to the crimes under investigation;
f. evidence of the attachment to the DIGITAL DEVICE of other storage devices or similar containers for electronic evidence;
g. evidence of programs (and associated data) that are designed to eliminate data from the DIGITAL DEVICE;
h. evidence of the times the DIGITAL DEVICE was used;
i. passwords, encryption keys, and other access devices that may be necessary to access the DIGITAL DEVICE;
j. documentation and manuals that may be necessary to access the DIGITAL DEVICE or to conduct a forensic examination of the DIGITAL DEVICE;
k. records of or information about Internet Protocol addresses used by the DIGITAL DEVICE; and
l. records of or information about the DIGITAL DEVICE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

20. With respect to any and all electronically stored information in cellular telephones and cellular devices, in addition to the information described herein, agents may also access, record and seize the following:

a. Telephone numbers of incoming/outgoing calls stored in the call registry;
b. Digital, cellular and/or telephone numbers and/or direct connect numbers, names and identities stored in the directories;
c. Any incoming/outgoing text messages relating to the above criminal violations;
d. Telephone subscriber information;

e. The telephone numbers stored in the cellular telephone and/or PDA;
f. Records relating to the use, possession, and control of any cellular telephones and cellular devices seized;
g. Any other electronic information stored in the memory and/or accessed by the active electronic features of the digital or cellular telephone including but not limited to photographs, videos, e-mail, and voice mail relating to the above TARGET OFFENSES.

21. Contextual information necessary to understand the evidence described in this attachment.

II. AUTHORIZED SEARCH PROCEDURE FOR DIGITAL DEVICES

1. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location.

2. In order to search for the items described above that may be maintained in electronic media, the search team are authorized to search, copy, image and seize the following items for off-site review:
   a. Any computer or storage medium capable of being used to commit further or store evidence of the TARGET OFFENSES; and
   b. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer or storage medium;

3. Pursuant to Rule 41(f)(1)(B), the government will retain a copy of the electronically stored information that was seized or copied for the purpose of the evidentiary authentication and any potential discovery obligations in any related prosecution.

4. This warrant does not cover the search and seizure of any Digital Devices determined by agents to be used exclusively by third parties not involved with the TARGET OFFENSES.

III. BIOMETRIC ACCESS TO DEVICES

During the execution of the search of the TARGET PREMISES and TARGET VEHICLE described in Attachment A-1, A-2, and A-3 law enforcement personnel are also specifically authorized to compel SANTIAGO to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

(a) any TARGET PHONE found at the TARGET PREMISES or in the TARGET VEHICLE, and

(b) where the TARGET PHONE is limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offenses as described in the search warrant affidavit and warrant attachments, for the purpose of attempting to unlock the TARGET PHONE's security features in order to search the contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to compel any other individuals found at the TARGET PREMISES to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any TARGET PHONE. Further, this warrant does not authorize law enforcement personnel to request that SANTIAGO to state or otherwise provide the password or any other means that may be used to unlock or access the TARGET PHONE, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the TARGET PHONE.

ATTACHMENT B-4

I. ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as a means of committing a criminal offense, namely violations of 21 U.S.C. § 841(a)(1); and conspiracy to possess with intent to distribute and/or distribute controlled substances, in violation of 21 U.S.C. § 846 ("TARGET OFFENSES").

a) Any CELLULAR DEVICE/ TELEPHONE which itself or which contains evidence, contraband, fruits, or instrumentalities of the TARGET OFFENSES, and forensic copies thereof.

b) Any controlled substances or controlled substance analogue;

With respect to any cellular device/telephone containing evidence falling within the scope of the foregoing categories of items to be seized;

1. evidence of who used, owned, or controlled the cellular device/telephone at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
2. evidence of software that would allow others to control the cellular device/telephone, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
3. evidence of the lack of such malicious software;
4. evidence indicating how and when the cellular device/ telephone accessed or used to determine the chronological context of device's access, use, and events relating to the crimes under investigation and to the phone user;
5. evidence indicating the cellular device's/telephone user's knowledge and/or intent as it relates to the crimes under investigation;
6. evidence of the attachment to the cellular device/telephone of other storage devices or similar containers for electronic evidence;
7. evidence of programs (and associated data) that are designed to eliminate data from the device;
8. evidence of the times the cellular device/telephone was used;

9. passwords, encryption keys, and other access devices that may be necessary to access the cellular device/telephone;
10. records of or information about Internet Protocol addresses used by the cellular device/telephone and
11. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
12. With respect to any and all electronically stored information in the cellular device/s/telephone, in addition to the information described herein, agents may also access, record and seize the following:
    i. Telephone numbers of incoming/outgoing calls stored in the call registry;
    ii. Digital, cellular and/or telephone numbers and/or direct connect numbers, names and identities stored in the directories;
    iii. Any incoming/outgoing text messages relating to the above criminal violations;
    iv. Telephone subscriber information;
    v. The telephone numbers stored in the cellular telephone and/or PDA;
    vi. Records relating to the use, possession, and control of any cellular devices/ telephones seized;
    vii. Any other electronic information stored in the memory and/or accessed by the active electronic features of the cellular phone/device including but not limited to photographs, videos, e-mail, and voice mail relating to the above TARGET OFFENSES.

As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on the cellular device/telephone and any forensic copies thereof.

II. AUTHORIZED SEARCH PROCEDURE FOR DIGITAL DEVICES

1. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location.

2. In order to search for the items described above that may be maintained in electronic media, the search team are authorized to search, copy, image and seize the following items for off-site review:
   a. Any computer or storage medium capable of being used to commit further or store evidence of the TARGET OFFENSES; and
   b. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer or storage medium;

3. Pursuant to Rule 41(f)(1)(B), the government will retain a copy of the electronically stored information that was seized or copied for the purpose of the evidentiary authentication and any potential discovery obligations in any related prosecution.

4. This warrant does not cover the search and seizure of any Digital Devices determined by agents to be used exclusively by third parties not involved with the TARGET OFFENSES.

III. BIOMETRIC ACCESS TO DEVICES

During the execution of the search of the TARGET PERSON described in Attachment A-4, law enforcement personnel are also specifically authorized to compel SANTIAGO to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

(a) any TARGET PHONE found on the TARGET PERSON, and

(b) where the TARGET PHONE is limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offenses as described in the search warrant affidavit and warrant attachments, for the purpose of attempting to unlock the TARGET PHONE's security features in order to search the contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to request that SANTIAGO to state or otherwise provide the password or any other means that may be used to unlock or access the TARGET PHONE, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the TARGET PHONE.